ECUTEL®

State of Utah

Networking System for Application Persistence
Solicitation # DG 4009
Proposal for Viatores^{TM} Mobility Software

July 7, 2004

Kevin Hayes
Vice President – Government Services

ECUTEL SYSTEMS, INC.
2300 Corporate Park Drive - Suite 410
Herndon, VA 21071
571-203-8335

2.3 Letter of Transmittal

ECUTEL®

July 7, 2004

Ms. Debbie Gundersen
State of Utah
Division of Purchasing
State Office Building, Room 3150
Salt Lake City, Utah 84114

Dear Ms. Gundersen:

Ecutel Systems, Inc. is pleased to respond to the State of Utah's Request for Proposal for the Networking System for Application Persistence. Ecutel is responding to the RFP with a proposal based on its Viatores Mobile VPN solution, which enables the seamless, secure integration of multiple networks.

The State of Utah faces significant challenges – leveraging emerging wireless technologies that enhance the productivity of its employees, ensuring the security and availability of network resources, while controlling operational costs.

Our objective is to help the State of Utah achieve its operational and financial goals by providing a mobility solution that enables seamless, secure roaming across today's disparate wired and wireless networks, as well as future commercial and Wi-Fi wireless network technologies. This proposal illustrates how the Ecutel Viatores mobility solution can meet these objectives.

I will serve as the authorized representative of Ecutel Systems, Inc. for all matters relating to this proposal. I have included my contact information for your convenience:

Name:	Kevin Hayes
Title:	Vice President – Government Services
Address:	2300 Corporate Park Drive – Suite 410 Herndon, VA 20171
Office Phone:	571-203-8335
Cellular Phone:	703-850-8963
Facsimile:	571-203-8310
Email:	khayes@ecutel.com

We appreciate the opportunity to submit our proposal and look forward to the success of your project.

Sincerely,

Kevin Hayes

2.4 Executive Summary

Background
With more than 22,000 employees, the State of Utah ranks as one of the largest employers in Utah. Like many large organizations, the State has determined that emerging wireless technologies and networks have the potential to significantly improve employee productivity, change the way employees work, and deliver a substantial return on investment.

The State has issued a Request for Proposal for a Networking System that will enable state employees to access applications located on the enterprise network from a variety of disparate networks, both wired and wireless.

Project Requirements
The State intends to establish a statewide contract for a solution that can be deployed throughout the State to enable employees to roam between service providers, and across multiple networks, while maintaining a persistent connection to their applications and network resources.

This network solution must provide diverse network connectivity, support for multiple carriers, session persistence when moving from one network, segment, connection media, or ISP to another, and maintaining application sessions without interruption.

Proposed Solution – Ecutel's Viatores Mobility Software

Ecutel Systems, Inc. is a leading provider of secure, mobility software to the enterprise and government markets. Ecutel's proposed solution, based on its Viatores Virtual Private Network (VPN) software, will enable State of Utah employees to remain continuously connected to their enterprise network and applications, **seamlessly**, **securely**, and **over any network**.

Ecutel is uniquely qualified to support this project with our differentiated solution:

Seamless Roaming The State of Utah requires persistent, continuous access to the enterprise across a variety of network technologies. Ecutel's solution will enable the State to integrate all of its existing LAN, WLAN, and ISP networks, and present a single, seamless network to its users. Employees will be able to access their applications and network resources without interruption as they move from one network to another.

Network Security Ecutel's Viatores software is the first mobility solution based on IPsec, the industry standard for security at the network or packet-processing layer of network communication. This standard is trusted and deployed by government agencies and commercial enterprises around the world.

In addition, Viatores centralized management capabilities will ensure that the State's network security policies can be enforced at all times, without the risks associated with solutions that require participation or compliance by end-users.

Standards-based Architecture Ecutel's Viatores software is the only solution based on trusted IETF standards, Mobile IP and IPSec. This is a critical differentiator from other proprietary software solutions. Because of its standards-compliant architecture, Viatores is not only compatible with all of the State's current network technologies and operating systems (Windows, Linux and Novell), but will easily support future technologies as well. This approach minimizes risk and ensures that the State's investment will be in a long-term solution.

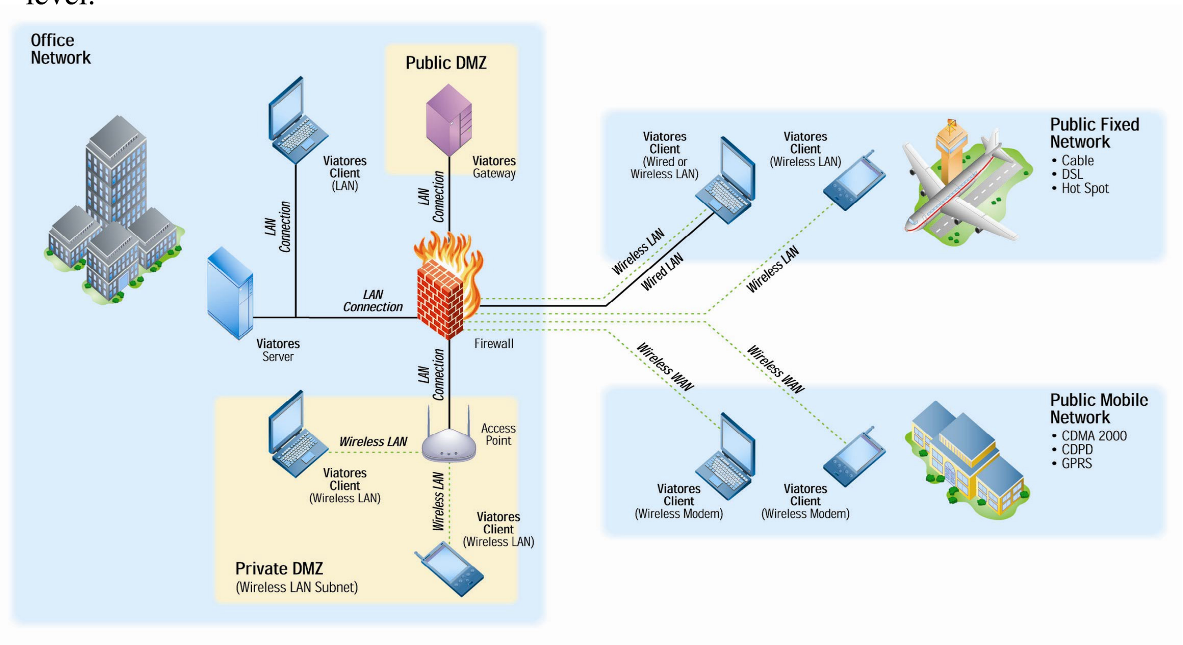
Centralized Administration and Reduced Management Costs In today's economic environment, the focus is on controlling operating costs and improving efficiencies. The proposed Viatores mobility solution can be centrally managed with fewer resources, and at a lower cost, while minimizing end-user calls to Help Desk support.

Proven Technology Ecutel's Viatores software is tested, certified, and sold by some of the leading technology firms in the world, including Hewlett-Packard, Siemens Business Services, and Matsushita. Viatores mobility software has been successfully implemented in a variety of commercial enterprises and government agencies.

Viatores Mobility Solution

Viatores is designed to enable mobile computers users to seamlessly roam across heterogeneous networks – whether wired or wireless - while maintaining data security (security and integrity) and persistent and bi-directional communications with peers.

The following illustration depicts the proposed Viatores mobility solution at a summary level.



Artwork © 2002 Network Diagram Solutions

The Viatores architecture consists of 4 major subsystems and components operating in a Client and Server mode. The subsystems and components are designed to be portable, run on multiple operating systems, and adhere to IETF communication and security standards.

Viatores Server

This main subsystem resides in a designated main or enterprise home mobile network. It functions as Mobile IP mobility server, VPN security server, IP packet attraction proxy, and tunneling router.

Viatores Client

This is mobile node or mobility client subsystem. It functions on a mobile device such as laptop computer, or handheld Personal Data Assistant (PDA). It operates as a mobility endpoint to receive and transmit tunneled IP packets between the current attached location and the assigned network's Viatores Server.

Viatores Gateway

This is a surrogate mobility subsystem for the Viatores Server. It functions as a Mobile IP router/tunneler between the private network and a public network, and operates with a boundary gateway device such as the firewall.

Viatores Manager

This is the configuration and administration subsystem. This subsystem enables the network administrator to define and manage security and mobility policies, centrally manage and provision servers and clients, and update server policies dynamically without interference.

2.15 References

#1 Company:	Siemens	
Address	Oslo, Norway	
Contact	Jan T. Herstad	IT Architect, CIO Office Scandinavia
Phone	+47 22-633-000	
Email	Email jan.herstad@siemens.com	

#2 Company	Transaction Network Services (TNS)	
Address	Reston, VA	
Contact	Curtis Generous	CTO
Phone	+1 703-453-8300	
Email	Curtis.Generous@tnsi.com	

#3 Company	Santa Clara Police Department	
Address	Santa Clara, CA	
Contact	Lt. Roger Luebkeman,	IT Director
Phone	+1 408-615-4718	
Email	rluebkeman@ci.santa-clara.ca.us	

#4 Company	Matsushita Electric Works	
Address	Tokyo, Japan	
Contact	Dr. Hiroshi Shimizu	General Manager
Phone	+81-3-3452-3390	
Email	shimizu@trc.mew.co.jp	

#5 Company	City of Honolulu	
Address	Honolulu, HI	
Contact	Alvin Sunahara	IT Director
Phone	+1 808-527-5830	
Email	asunahara@co.honolulu.hi.us	

2.17 Ecutel Systems, Inc. Information

2.17.1 Product Technology

Ecutel Systems Inc. is the leading provider of advanced mobile networking software enabling secure, real-time communications for the mobile workforce. The Viatores Mobile VPN (Virtual Private Network) is the only software-based mobility solution that incorporates two IETF standards, Mobile IP and IPSec, to enable mobile computer users to seamlessly roam across heterogeneous networks – whether wired or wireless - while maintaining both data security and persistent and bi-directional communication.

Ecutel's solutions change the way people work by giving today's mobile professionals the freedom to roam the world and communicate securely anytime, anywhere, over any network, in real-time. Ecutel's Viatores software is sold by some of the leading technology firms in the world, including Hewlett-Packard, Siemens Business Services, and Matsushita. Ecutel is a privately held company headquartered in Herndon, VA.

Viatores Mobile VPN Solution- Simplicity, Security, Mobility and Optimized Roaming

- Trusted security of IPSec and other proven standards including RSA, DSA, AES, 3DES, SHA, and PKI

- Seamless roaming and application persistence using Advanced IP mobility, including support for public and private addresses, static mobile IP addresses, network traversal, and location discovery support

- Automatic selection of best available network

- Optimized and policy-driven security

- Single sign-on and SecurityFirst™ network login

- Integration with existing applications and network infrastructure

- Vendor-independent security solution allows interoperability between the different hardware vendors

- Support for all wireless networks: Wi-Fi, GPRS, 1xRTT, CDPD, and other networks

- Scalable and flexible architecture to support the growing number of mobile devices and network infrastructures

Viatores Mobile VPN Components

Viatores Server

The Viatores Server is the core server component of the Viatores system. It resides within the corporate network and is responsible for several tasks including encryption, authentication, Mobile IP addresses, and traffic management.

Viatores Gateway (Price included with Server Module)

The Viatores Gateway provides a flexible and portable mechanism for secure traversal of firewalls. It verifies traffic directed before forwarding it across the firewall to the Viatores Server to authenticate.

Viatores Manager (Price included with Server Module)

The Viatores Manager is a component used by network and system administrators for user management, key management, and policy distribution. This component can reside on any secure machine and can deploy the configuration details to the Viatores Server and the individual Clients.

Viatores Client

The Viatores Client is the only software necessary on the mobile device. It is responsible for all the functions required by the client including the network device discovery, communication with the server components, authentication, and encryption/decryption

Hardware Acceleration PCI cards

The Viatores Server supports an optional PCI hardware acceleration card. The acceleration card is designed to offload CPU-intensive encryption functions from the host server to improve overall performance and throughput. Using hardware acceleration, the throughput of the Viatores Server can be increased three- to four-fold. You can purchase an acceleration card directly from Ecutel or from an Ecutel authorized reseller. The Viatores Server supports two acceleration cards: SafeXcel™ 241-PCI and SafeXcel™141-PCI.

Ecutel Differentiation

There are many products that attempt to address the problems of mobility, seamless switching and application persistence. Ecutel's Viatores solution is uniquely differentiated in the following ways:

Standards-based Solution Ecutel's Viatores software is the only solution based on trusted IETF standards, Mobile IP and IPSec. This is a critical differentiator from other proprietary solutions. Because of Viatores' standards-compliant architecture, our solution optimizes mobility without compromising network security. The Internet Standards Process defines the nature and process of Internet standards. This process highlights the importance of following standards and the pitfalls for not doing so. In the world of heightened security, adhering to standards reduces the risks associated with proprietary solutions, which are architected by a handful of individuals and tested by a few. True testing takes place in customer networks with real-world data and many consequences. When it comes to networking security, the standard of choice is IPSec!

Operating Systems Compatibility Viatores was designed independent of any specific operating system security features and, hence, it is portable to multiple operating systems. This makes Viatores less vulnerable to exploitations of weaknesses specific to any operating system.

Support for Existing Applications and Network Architecture Viatores supports your organization's existing infrastructure. Whether you are using Active Directory, RADIUS, Novell, LDAP, or RSA SecurID; Viatores will take advantage and interoperate with your backend network infrastructure.

Proven Technology Viatores has been successfully implemented in a variety of Fortune 100 enterprises and government agencies, with implementations ranging from 25 users to several thousand per installation. In addition, Viatores is branded and sold worldwide by several global resellers under the following brands: Siemens Mobilis, HP Open Roaming, and Matsushita NetCocoon.

Scalability. Viatores is designed to work in any environment, regardless of its size with unique features such as cryptographic hardware acceleration, server clustering, and support for primary and secondary backend authentication severs.

Network Management Agency system administrators will be able to use the Viatores Manager to control the Viatores Server from a workstation or their desktop. They will not be bound to the server room when doing maintenance on the server. Redundant failover servers can be configured so even if your server goes down, secure mobile communications do not.

Remote Management Tool Ecutel provides an optional remote management solution, which gives network administrators the ability to control the Viatores Server remotely using a Blackberry or other handheld PDA.

Modem Agnostic Our solution does not require the use of any specific brand of modems for optimized performance. You can use any brand modem, from Airlink to Sierra Wireless. Other solutions may tie you to a specific brand of modems, which could have an impact on the overall cost of the solution.

Network Switching by Policy In addition to selecting the best available bandwidth, Viatores gives network administrators full control over the network adapter prioritization so that the policy is determined by any factor relevant to the agency.

Security Ecutel offers a true VPN solution that exceeds traditional VPN standards. And unlike other solutions on the market, our solution does not require opening firewall ports to the public. The Viatores Gateway component is designed to authenticate user requests outside the firewall before allowing users inside. This ensures that no unauthorized users are allowed inside the firewall. Our business began by doing work for the Department of Defense and the DEA, security has will continue to be our highest priority.

2.17.2 Services

Installation (Optional)

Ecutel offers software installation and configuration services to its customers. Although Ecutel designed the Viatores platform to be intuitively and easily installed by system administrators, an agency may not have the manpower or resources to install on their own. Our project engineers, who have extensive experience in the installation of Viatores, easily address the many variables in each installation, including configuration and network requirements.

Training (Optional)

Viatores Basic Technical Training course: Provide an overview of networking protocol standards (MIP, IPSec, Routing, DHCP, PPP, Wired and Wireless protocols); Viatores components; Viatores mobility, security and connectivity capabilities; Administrator and User configuration, product installation preparation; hands-on class room practice. This course will be taught by an engineer with minimum of 7 years experience.

Consulting (Optional)

Ecutel Systems, Inc. engineers are available to you on a consultant basis on a variety of services including network design, security assessment, and post deployment evaluation. Our engineers, who have extensive wireless and wired network experience, can help individual agencies overcome the pain in deploying and maintaining these networks.

Geographic Territory Covered

Professional Services (i.e. installation, training and consulting) are available throughout the entire state. However our service fees do not include travel and other expense. All travel will be invoiced at cost based on travel from our Virginia office. With any Purchase Order over $25,000, the travel fee will be waived for professional services for the first site visit.

2.17.3 Technical Support

Technical support coverage is offered during normal business hours 9:00 AM through 5:00 PM EST. 24 X 7 support is available at additional fee.

Standard Support Subscription

- Web, email, and phone support direct to customers provided by Ecutel.
- 9 to 5 (business days) support through web, email and phone.
- 4 designated customer contacts are registered with Ecutel
- Problem assigned to support engineer within 4 hours
- Unlimited number of support incidents
- Maintenance Subscription is required.

All incoming software trouble reports are first logged into the support/help desk database and assigned with a tracking number and severity level, which could be Catastrophic, Critical, Major, Normal and Minor. The support team identifies whether the reported problem is related to Ecutel product or to the environment. If the issue cannot be resolved over the phone or email within a time period allocated to the critical level, the development team is consulted and engaged for a solution such as a workaround procedure, IP network monitoring, a software fix, or an on-site support visit. Critical level is escalated to the next level as the condition requires as follows:

- Catastrophic: Immediate attention and support answer is provided within 4 hours. Continuous monitoring is performed by the help desk staff and designated development engineers.
- Critical: Immediate attention and support answer is provided within an 8 hour period. Daily report by the help desk on the status with daily monitoring by the help desk staff and designated development engineers.
- Major: Support answer is provided within 24 hour period. Report every 2 days by the help desk support staff.
- Normal: Phone and email support answer is provided within a 24-72 hour period. Report is generated every 3 days by the help desk staff
- Minor: Support answer is provided over the phone or email without escalation.

The help desk staff updates the support database to reflect the support level changes and also store the actual remedial procedures and software fixes as they are sent to the agency.

Support Contact Information
Ecutel Systems, Inc.
2300 Corporate Park Drive Suite 410
Herndon, VA 20171
Main Office 571-203-8300
Fax 571-203-8310
Email: support@ecutel.com
Fax: 571-203-8310

Primary Support Contact:	Mark Mazur	Project Engineer	571-203-8321
Backup Support Contact:	Gowri Makineni	System Engineer	571-203-8329

Billing Inquiries
All questions regarding billing shall be directed to the contact below. A response shall be expected within 1 business day.

Thomas Egan	CFO	571-203-8334	tegan@ecutel.com

4.0 Guarantees

4.1 Warranty

4.1.1 The vendor shall agree to warrant and assume responsibility for the system and/or related services purchased under this contract.

Ecutel Response: Agreed

4.1.2 If, because of design defects, the system supplied requires modifications, repair, or replacement, the vendor shall promptly provide the necessary solution to the State at no expense to the buyer.

Ecutel Response: Agreed

4.1.3 In all cases the vendor agrees to replace or repair any defective components of the system during the warranty period.

Ecutel Response: Agreed

4.1.4 Any vendor unable to provide local service must clarify how they intend to provide satisfactory service support comparable to a local service center.

Ecutel Response: Agreed, Ecutel Systems, Inc. can offer local support.

4.2 Maintenance

4.2.1 The vendor shall provide the names, titles, addresses, and telephone numbers of the primary and backup contacts for service problems.

Ecutel Response:
Support Contact Information
Ecutel Systems, Inc.
2300 Corporate Park Drive Suite 410
Herndon, VA 20171
Main Office 571-203-8300
Fax 571-203-8310
Email: support@ecutel.com
Fax: 571-203-8310

Primary Contact:	**Mark Mazur**	**Project Engineer**	**571-203-8321**
Backup Contact:	**Gowri Makineni**	**System Engineer**	**571-203-8329**

4.2.2 The vendor shall present an escalation procedure for service problems, along with time lines for escalation.

Ecutel Response: All incoming software trouble reports are first logged into the support/help desk database and assigned with a tracking number and severity level, which could be Catastrophic, Critical, Major, Normal and Minor. The support team identifies whether the reported problem is related to Ecutel product or to the environment. If the issue cannot be resolved over the phone or email within a time period allocated to the critical level, the development team is consulted and engaged

for a solution such as a workaround procedure, IP network monitoring, a software fix, or an on-site support visit. Critical level is escalated to the next level as the condition requires as follows:

- **Catastrophic: Immediate attention and support answer is provided within 4 hours. Continuous monitoring is performed by the help desk staff and designated development engineers.**
- **Critical: Immediate attention and support answer is provided within an 8 hour period. Daily report by the help desk on the status with daily monitoring by the help desk staff and designated development engineers.**
- **Major: Support answer is provided within 24 hour period. Report every 2 days by the help desk support staff.**
- **Normal: Phone and email support answer is provided within a 24-72 hour period. Report is generated every 3 days by the help desk staff**
- **Minor: Support answer is provided over the phone or email without escalation.**

The help desk staff updates the support database to reflect the support level changes and also store the actual remedial procedures and software fixes as they are sent to the agency.

4.2.3 The vendor shall state its standard policy for response time and repair, including emergency or priority services.

Ecutel Response: See Catastrophic and Critical levels of support described in section 4.2.2 above.

4.3 Training

4.3.1 The vendor shall provide details on course material that is offered, and whether training can be provided at a State facility.

Ecutel Response:

Viatores Mobile VPN Fundamentals

Duration: 2 Day

Delivery Method: Classroom and Laboratory

Skill Level: Basic

Overview:

Develop the knowledge and skills you need to describe, configure, verify, troubleshoot, and manage the mobility and security features in the Viatores Mobile Virtual Private Network (mVPN) product family.

Who Should Take This Course:

- **Technical individuals who implement and maintain mobility and security product solutions.**

What is Taught:

- **Overview of the Viatores components and their functions**
- **Basic design principles for a Viatores mobility solution**
- **Overview of the standards and terminology used by the Viatores components**

- **Pre-installation steps and procedures**
- **Installation of the Server, Client, and Gateway**
- **Configuration of a multi-faceted Viatores mobility solution**
- **Administration of the Viatores server and client components**
- **Basic troubleshooting of the Viatores components**

Prerequisites:

The student should understand and be familiar with Virtual Private Networks (VPNs) and Mobile IP. Students should also have basic knowledge of the Windows 2000 and XP operating system and be familiar with networking and security terms and concepts. Students should have basic knowledge of Wireless LAN (WLAN) implementation and operation.

4.3.2 Vendors should describe what technical instructor lead training they offer. The costs for this training should be provided in the Pricing Section of the RFP using two different venue assumptions:

a. Vendor Facility

b. State of Utah Facility

Ecutel Response: See Description below for description and pricing has been included in Section 6

Advanced Viatores Mobile VPN Training

Duration: 3.5 Days

Delivery Method: Classroom and Laboratory

Skill Level: Advanced

Overview:

Develop the knowledge and skills you need to describe, configure, verify, troubleshoot, and manage user authentication and other advanced features in the Viatores Mobile Virtual Private Network (mVPN) product family.

Who Should Take This Course:

- **Technical individuals who implement and maintain mobility and security product solutions.**
- **Technical trainers who wish to train other staff on the Viatores Mobile VPN solution.**

What is Taught:

- **In depth exploration of the Viatores components and their functions**
- **Basic design principles for a Viatores mobility solution to include integration with legacy user authentication systems**
- **Review of the standards and terminology used**
- **Pre-installation steps and procedures for large-scale deployments**
- **Installation of the Server, Client, and Gateway components**
- **Configuration of a multi-user Viatores mobility solution**
- **Advanced troubleshooting of the Viatores components**
- **Configuration of the Viatores solution for use with 3rd party authentication servers (X.509 Certificates, RADIUS, RSA SecurID, MS Active Directory, and LDAP)**
- **Administration of the Viatores system as integrated with legacy authentication systems.**

Prerequisites:

Students should also have basic knowledge of the Linux, Windows 2000 and XP operating systems and be familiar with networking and security terms and concepts. Students should have basic knowledge of user administration using RADIUS, LDAP, and Microsoft Active Directory.

4.4 Technical Manuals

4.4.1 The vendor shall describe the technical manuals or on-line technical information that will be provided with each order.

Ecutel Response: The Viatores software is delivered with the following documents:

- **Viatores Administrator Manual - This document describes the following topics: Viatores architecture and components, pre-installation process, component installation, component configuration, management of various Viatores components, using SNMP to monitor, server cluster management.**

- **Viatores Client Manuals (for laptops and Pocket PC) - This document describes how to install, configure and use the Viatores with information on how user specific parameter is managed.**

- **Viatores Batch MSI Installation Guide - This document describes how to use the Viatores silent or batch installation program and how to supply parameters to automate client installation on XP and 2K mobile devices.**

- **Quick Start Guide**

- **Release notes**

- **Viatores Technical Notes**

- **Viatores FAQ (Frequently Asked Question)**

5.0 Technical Specifications

5.1 General

The State of Utah is building a wireless Ethernet environment using 802.11b technology and port level authentication based on IEEE 802.1x standards. This environment will be deployed enterprise-wide to the employees of the State of Utah, including executive branch agencies as well as other government organizations. This environment is designed such that the following major objectives will be accomplished:

a. Authentication of wireless users for authorized access.
b. Encryption of user credentials and data.
c. Scalable as an interoperable statewide enterprise solution available in State agency buildings and "Hotspots" at other locations.
d. Client software will integrate and work with various Authentication/Authorization Directories (LDAP, NDS, Web Services, etc.).

The proposed architecture will involve access point 802.11 radios that in most instances will be a Cisco product. These radios will use a version of Cisco Internetworking Operating System (IOS) compatible with routers, switches, and related Cisco equipment in use as part of the State WAN. Using IOS, these devices can be configured to restrict access based on access control lists (ACLs). Administrative authorization will be directed to a Cisco ACS access server. The ACS server will interface with the LDAP-compliant, Utah Master Directory (UMD), 802.11b access points, and with other Cisco network equipment currently in use. The following sections address specific requirements for vendor client software solicited under this RFP.

5.2 802.1X Compliance (Mandatory)

The client software must be IEEE 802.1x compliant, WPA compatible, and include the ability to provide seamless connectivity using any 802.1x-compliant, 802.11.a, .b, or, .g, wireless card, or built-in PC wireless electronics. Vendors should explain how their product meets these criteria.

Ecutel Response: The Ecutel's Viatores solution complies with the 802.1X requirement.

The Viatores mobile VPN Client software operates at the IP layer-3 and higher in the mobile device's operating system and therefore can layer above and interoperate with any IP based layer-2 communication interfaces available for communication such as wired LAN, wireless WAN (such as CDMA, EDGE, GPRS, EVDO, IPMobileNet, etc) and wireless LAN (such as 802.1a, 802.1b, 802.1g with 802.1X and WPA authentication). The Viatores Client driver is an NDIS dynamic protocol binding driver which can bind to all Microsoft NDIS and Miniport interfaces on the mobile devices. It is capable of providing packet control, filtering, and management over any communication interfaces using standard operating system interface calls.

When the 802.1x capable wireless LAN card is configured to operate in the IEEE 802.1X or WPA authentication mode, it is necessary that its driver can successfully exchange 802.1X authentication traffic (such as EAP-TLS, EAP-TTLS frames, etc) with the wireless LAN access point with matching SSID to authenticate and derive encryption key from the back-end EAP RADIUS server before it can gain access to the wireless network.

The Viatores Client protocol driver is capable of recognizing such inbound and outbound 802.1X encoded Ethernet frames and forwarding them to the wireless network when the 802.1X client driver generates authentication traffic with an access point. The Viatores driver inspects each Ethernet frame to look for an Ethernet 802.1X authentication Type code of 0x888e (in Hexadecimal value) after the Destination and Source MAC address fields.

After the 802.1X authentication sequence is completed, the 802.11 wireless card will successfully associate with the access point. At this point, the Viatores Client will receive a successful event status of a wireless network card attachment to an access point from the operating system and obtains a DHCP IP address for its use.

After a DHCP IP is assigned to the wireless card, the Viatores Client will generate proper Mobile IP and IPSec traffic to its designated Viatores Server to inform its current wireless LAN attachment IP address (also known as care-of address) and continues to maintain the tunneled session between the laptop and its enterprise network.

Due to the flexibility of Viatores' rule-based network access policy implemented along with the standard Mobile IP protocol, Viatores Client roaming is automatic and more importantly seamless over any available IP based wired or wireless network connections configured with or without 802.1X authentication.

Figure 5-2 shows that Ethernet packets from the 802.1X driver flow through the Viatores driver during the period of 802.1X authentication between the mobile device and the wireless access point. The Viatores Client is capable of processing 802.1X traffic and therefore is compliant with the 5.2 requirement.

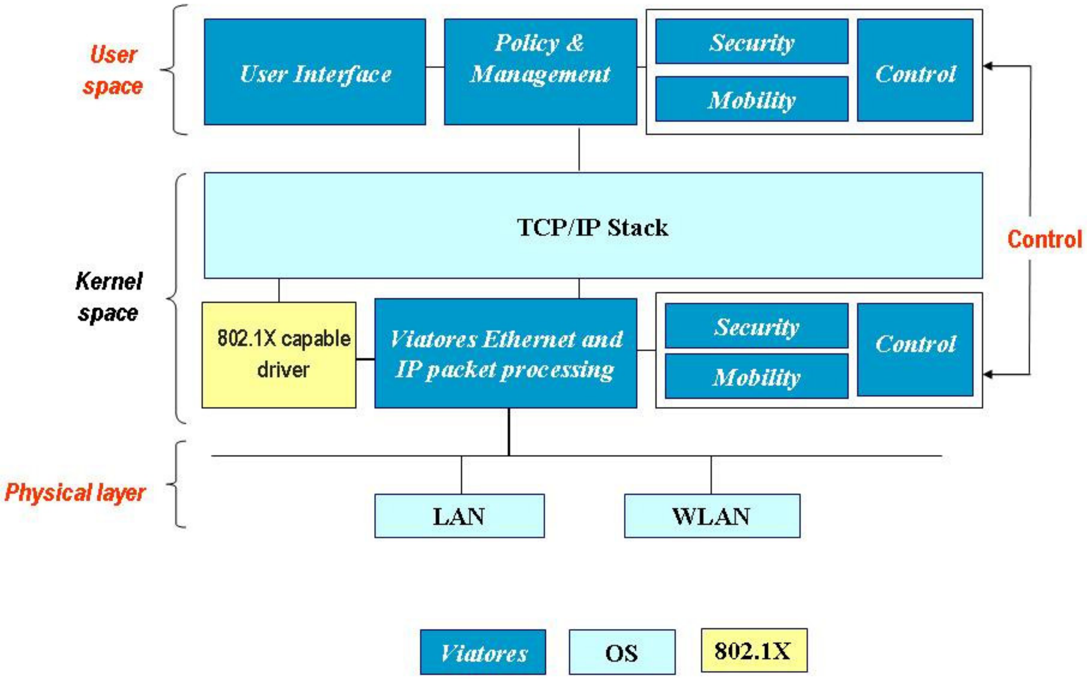


Figure 5-2 : Viatores mobility and security driver recognizes 802.1X Ethernet traffic to enable pass-through.

5.3 EAP over LAN Capable—-(Mandatory)

The vendor solution must be capable of the IEEE standard for 802.1x port-based access control. The client software must be capable of adding EAPOL (EAP over LAN) data to the MAC header of the Ethernet frame (compliant with IEEE 802.1x standards). Vendors should explain how their product meets these criteria.

Ecutel Response: The Ecutel's Viatores solution complies with the EAP over LAN requirement.

The Viatores Client solution is compatible with 802.1X compatibility using one or both of the following approaches:

- **Built-in operating system driver with 802.1X capability (for example: Microsoft XP and 2000)**
- **3rd-party driver software with 802.1X capability for the Microsoft XP, 2000, ME, 98, and CE, etc from either Meetinghouse (www.mtghouse.com) or Funk Software (www.funk.com) software vendors.**

These built-in 802.1X, WPA and 3rd-party drivers are capable of processing and adding EAP data fields to the Ethernet packets. The Viatores driver facilitates pass-through of EAPOL traffic as it detects them across LAN and WLAN interfaces.

The Viatores Client can co-exist with 802.1X products that are capable of generating EAP over LAN traffic, therefore it is compliant with the 5.3 requirement.

5.4 Existing 802.11 Equipment Support—-(Mandatory)

Does the software work with Cisco 802.11 radios and Enterasys 802.11 radios? Vendors should explain how their product meets these criteria.

Ecutel Response: The Ecutel's Viatores solution complies with the State of Utah's existing 802.11 equipment support requirement

Yes, the Viatores Client interoperates with Cisco 802.11 and Enterasys 802.11 radios. Because Cisco and Enterasys products come with NDIS drivers, these drivers can be installed and layered with the Viatores driver as depicted in figure 5.2. After both drivers are loaded, the Viatores Client can provide the following functions to enable seamless use of the device on the wireless network.

- **NDIS binding and passing information according to the standard specification**
- **Perform DHCP request and response to acquire network IP address, netmask and router IP.**
- **Maintain route entry table to associate IP routing information with all IP interfaces**
- **Recognize Plug-and-Play and card hot swapping events when the LAN or wireless LAN card is inserted or removed.**
- **Recognize network card events when the wireless LAN attaches to or detaches from a wireless access point**
- **Display all wireless LAN cards on the device in the Viatores Client to allow viewing and even setting to a specific static IP address if the deployment network does not provide DHCP services.**
- **Allow ranking of roaming preference between LAN, wireless LAN and other connection types, and even between multiple wireless LAN interfaces.**
- **Discern standard Ethernet frames and EAP-enabled Ethernet frames to perform proper manipulation and filtering.**

By providing interfaces to NDIS and operating system interfaces, the Viatores Client can work with Cisco and Enterasys 802.11 radios , in addition to a variety of other commercially available 802.11 products, and therefore is compliant with the 5.4 requirement.

5.5 802.11 Equipment Support—-(Mandatory)

Vendors should explain, in detail, which 802.11 vendor equipment that they know to be not compatible with, or supported by, their software.

Ecutel Response: The Ecutel's Viatores solution complies with the 802.11 equipment support requirement

The Viatores Client has been tested and proven to work with a large number of popular 802.11 wireless cards and access points from major vendors for operating systems such as XP, Win2000, 98, ME and PocketPC. For the laptop operating systems, the Viatores Client interoperates with 802.11 equipment from Cisco, Proxim, 3-COM, Enterasys, Linksys, Alvarion, Intel, D-Link, Netgear, Orinoco, Lucent, Aironet, and so forth. The Viatores software has been tested and interoperated in the following modes: 802.11, 802.11a, 802.11b, 802.11g, with and without 802.1X authentication modes.

Since there is a very large number of 802.11 cards with varying levels of NDIS compliance and configuration of the access point devices, Ecutel is currently aware of the following two incompatibility issues:

- **Pocket PC 2002 Linksys in compact flash format, the Viatores Client for PocketPC 2002 does operate fully with this card's driver.**
- **Proxim access point, Harmony model, when configured with control and tunnel mode over multiple subnets, may block and interfere with Viatores packet routing and tunneling.**

Nonetheless, Viatores' compatibility goal is to continue interoperability test with new 802.11 wireless cards and access points as they are available or used by our customers to ensure all access problems are identified early and resolved as quickly as possible for end users.

5.6 Compatible with Cisco ACS Version 3.2 and Higher—-(Mandatory)

The software must interface with Cisco ACS RADIUS services (version 3.2 and higher). Vendors should explain how their product meets these criteria.

Ecutel Response: The Ecutel's Viatores solution complies with the compatibility with Cisco ACS V 3.2 and higher requirement

There are two types of authentication interfaces afforded by the Ecutel solution:

- **Layer-2 authentication.**
- **User and Viatores network level authentications.**

The layer-2 authentication is performed by 3rd –party 802.1X drivers as described in section 5.2 above.

For the layer-3 and user authentication levels, the Viatores Server supports the following authentication protocols to interface to one or more authentication servers such as the Cisco ACS, using the following protocols:

- **RADIUS**
- **LDAP**
- **Microsoft Active Directory**
- **Public Key Certificate authority for X.509 validation**
- **Token based authentication server such as RSA SecurID**
- **Local user name and password**

After the layer-2 802.1X authentication is successfully performed or when the user starts the Viatores Client from a network other than the 802.1X network, the Viatores Client will prompt the user to provide authentication credential, encrypts it, and then sends it in a secure authenticated tunnel to the Viatores Server. When the Viatores Server receives it, it will validate against its mobile user records before eventually forwarding the credential to the destination authenticator server, such as the Cisco ACS, using standard RADIUS protocol in the form of Access-Request with encrypted password in a separate tunnel between the Viatores Server and the ACS RADIUS server.

When the Cisco ACS RADIUS server returns user authentication status in the form of Access-Accept or Access-Reject, the Viatores Server in turn encrypts it and returns to the Viatores Client to allow or deny user access to the network.

If there is no response from the main ACS RADIUS server within a pre-determined interval, the Viatores Server will resend a similar authentication Access-Request to an alternative ACS RADIUS server if so configured. When the RADIUS Access-Accept or Access-Reject status is returned to the Viatores Server, the Viatores Server subsequently forwards it to the Viatores Client.

In order to establish a secure path between the Viatores Server and ACS RADIUS server to authenticate mobile users, the system administrator can use the Viatores Manager to enter the following configuration parameters:

- **Define one or more user groups to be authenticated by RADIUS protocol. The system administrator can define as many groups as necessary**
- **Define one or more RADIUS authentication schemes, in which contains the following information:**
    - **IP address of the primary RADIUS compliant server**
    - **IP address of the fail-over RADIUS compliant server**
    - **RADIUS authentication Port number**
    - **RADIUS shared secrets for the main and back-up RADIUS servers**

The Viatores Server is very flexible by providing an unlimited number of RADIUS server scheme definitions to support concurrent authentication of large number of users to multiple RADIUS servers, therefore it is compliant with the 5.6 requirement.

5.7 Authentication Directories

In order to work with the State's directory system, it is highly desirable that the vendor provided software be compliant with PAP, which is a requirement for the interface with the LDAP-compliant Utah Master Directory (UMD). A list of authentication directories, such as LDAP, NDS, and Web services, with which the software is compatible, should be included. Vendors should explain how their product meets these criteria.

Ecutel Response: The Ecutel's Viatores solution works seamlessly with the PAP and LDAP protocols to authenticate user access to the enterprise network

Viatores Client works with PPP-based Remote Access servers, such as those provided by the Windows NT, Windows 2000 and public ISP Point-of-Presence, to allow mobile device to build a secure tunnel to the enterprise network, therefore it is necessary for the dial-up operation to select the "PAP option" within the dial-up manger to allow password to be forwarded unencrypted from the mobile device to the Access Server. and then ultimately forwarded to the UMD for authentication.

5.8 Encryption and Security—-(Mandatory)

Explain the product's method of data encryption, including all credentials and data passed before, during, and after the association with any 802.1x compliant 802.11 radio. Does the system provide VPN class security (encryption, authentication, and integrity) on the IEEE 802.11x network? Does the system connectivity solution support the following encryption and integrity protocols: 3DES, AES, MD5, PKI, SHA-1? Describe all security standards with which the product adheres, and the road map for adherence to new security standards and algorithms as they become available.

Ecutel Response: The Ecutel's Viatores solution complies with the encryption and security requirement

During the association time with the 802.11 network using 802.1X protocol, the mobile device 802.1X driver and the access point will exchange 802.1X traffic, which is based on user credentials such as user name, password or digital certificate. The 802.1X protocol allows a secure exchange of credential and keys using protocols such as 802.1X EAP-TLS or EAP-TTLS.

Viatores establishes a secure tunnel to authenticate the user and the mobile device after the 802.1X physical connection has been established.

Viatores' security strength is based on a combination of:

- **User level authentication**
- **Mobile IP authentication standard**
- **IPSec security and integrity standard**
- **Security state maintenance on both the Viatores Server and Gateway to allow only authenticated user's traffic to traverse the enterprise network.**

At the user level authentication, the user must provide either of the following to the Viatores Client:

- **User name and password – this is used to validated a distinct user, based on what the user memorizes, against the authenticator servers using LDAP, RADIUS, Active Directory protocol.**
- **2-factor authentication with token and PIN – this is used to validate what the user possess and what the user remembers against an authenticator server using RADIUS or SecurID protocol.**

For the first registration message, the Viatores Client will encrypt the user credential using 3-DES algorithm, places it into the payload extension of the Mobile IP registration packet, and then hashes the entire Mobile IP registration with a non-reversible MD-5 algorithm based on a shared secret according to the Mobile IP protocol.

The Viatores Client sends out Mobile IP registrations to the Viatores Server regularly or when the mobile device roams. For each Mobile IP registration, the packet contains new clock time value and a new computed MD-5 hash value to enable the Viatores Server to recognize the mobile client and maintain continuous tunnel states with the mobile devices. The Viatores Registration process ensures that only valid mobile user holding proper credential can establish communication path to the Viatores Gateway and Server.

After the Viatores Mobile IP state is authenticated, the mobile node will perform IPSec Internet Key Exchange (IKE) Phase-1, also known as IKE Main Mode phase, using Diffie-Hellman public/private key exchange algorithm, AES encryption and SHA-1 integrity algorithm to establish a secure tunnel to perform mutual Client and Server authentication based on either:

- **IPSec pre-shared secret**
- **Digital signature (such as RSA and DSA) using X.509 digital certificate configured on the mobile device**

If the mutual authentication option is selected to use public/private key based digital signature, the Viatores Server will interface to the Public Key Infrastructure (PKI)'s Certificate Revocation List (CA) and the Certificate Authority (CA) certificates to ensure the X.509 digital certificate to be authenticated has been properly signed by a trusted CA, has not been revoked and is still valid since the issuance date.

After the IKE Main Mode tunnel has been established, both sides will establish the IKE phase-2, also known as the Quick Mode phase. In this phase, both sides will perform an additional Diffie-Hellman public/private key exchange to create a new secure tunnel. In this new and second secure tunnel, the Viatores Client and Server will exchange additional cryptographic data to allow both sides to generate symmetric keys for IPSec packet encryption (i.e. for use with AES encryption algorithm) and packet integrity control (i.e. for use with SHA-1 algorithm).

After the IKE Quick Mode phase, both the Viatores Client and Viatores Server will have an end-to-end authenticated tunnel and states to perform the following operations on all IP packets:

- **Perform IP payload encryption using AES or 3-DES algorithm**
- **Compute IPSec packet header to provide tunnel IP identities and packet replay protection**
- **Compute an IPSec non-reversible hash checksum of the entire IPSec packet using SHA-1 algorithm**
- **Encapsulate the entire IPSec packet with Mobile IP header using the IP address authenticated during Mobile IP registration**

Due to the use of IPSec protocol, the Viatores system provides the following security benefits:

- **against IP packet forgery, tempering, packet replay during transmit;**
- **with strong packet encryption to protect sensitive information;**
- **Prevent key reuse by refreshing with new cryptographic keys regularly based on a pre-configured time interval parameters configured by the administrator.**

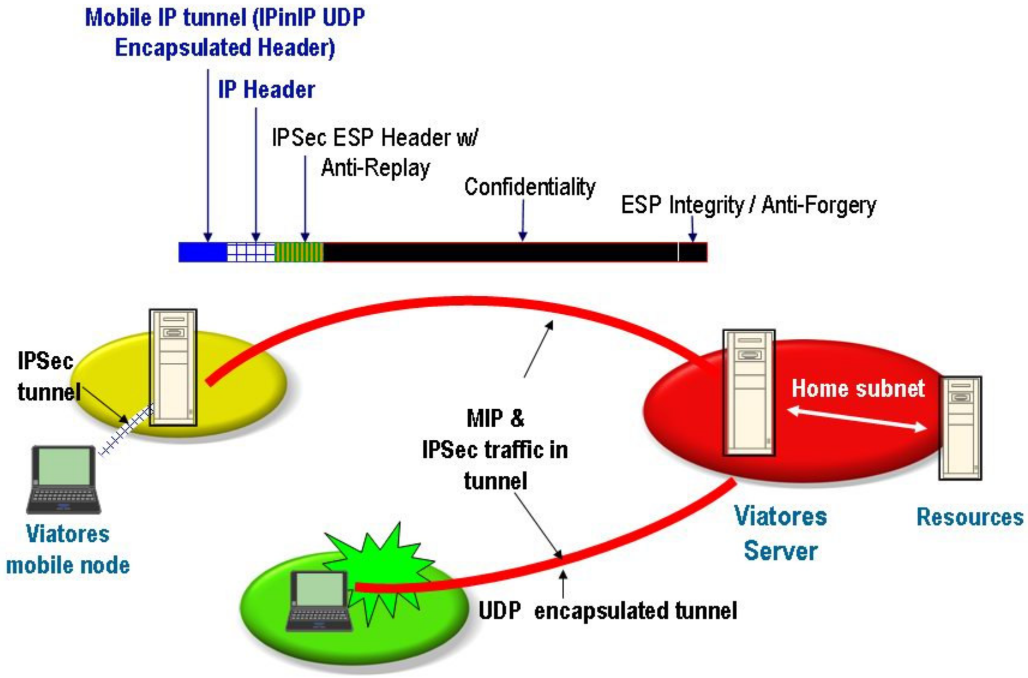

Mobile IP tunnel (IPinIP UDP Encapsulated Header)
IP Header
IPSec ESP Header w/ Anti-Replay
Confidentiality
ESP Integrity / Anti-Forgery
IPSec tunnel
Viatores mobile node
MIP & IPSec traffic in tunnel
Home subnet
Viatores Server
Resources
UDP encapsulated tunnel

Figure 5-8: Viatores secured tunneled traffic is protected with IPSec's Anti-Replay, Confidentiality and Anti-Forgery

More importantly, the Viatores Client maintains a fixed IP address on the mobile device and on the Viatores Server through the use of Mobile IP protocol, therefore the Client and Server can always maintain a persistent IPSec tunnel and allows it to remain secure as the mobile device switch from one network to another, between wired network and wireless networks. With a permanent IP address being maintained on the IP stack, the Client and Server applications can sustain network disruption (such as during Wi-Fi signal fading or roaming into or out of coverage, etc) thus enables maintaining secure end-to-end connections persistently.

In terms of security enhancement roadmap, Ecutel plans to provide multiple product improvements in the following areas:

- **Multiple and concurrent user authentication during log-on such as Microsoft Active Directory credentials, LDAP/SSL and SecurID.**
- **IETF Internet Key Exchange (IKE) version 2 which will be faster and more efficient, especially for slow speed networks.**

Ecutel feels strongly that Viatores security capability meets or exceeds the 5.8 requirements.

5.9 Cross Platform Compatibility—-(Mandatory)

The client software must work with as many of the following PC operating systems as possible: Any currently supported Windows operating system that has wireless capability (XP, 2000, CE, 98, and Millennium Edition), Linux, and Apple OS X. Vendors should explain how their product meets these criteria.

Ecutel Response: The Ecutel's Viatores solution complies with the cross platform compatibility requirement

The Viatores Client software currently operates on the following platforms:

- **Windows 98**
- **Windows ME**
- **Windows 2000**
- **Windows XP**
- **Pocket PC 2002/2003**

to communicate with the Viatores Server and Gateway operating in the following platforms:

- **Windows 2000 Server**
- **Windows 2003 Server**
- **Redhat Linux**

The Viatores Client and Server carry a similar architecture to support policy driven Mobile IP and IP Security functionality – see figure 5-9. The Viatores Client's architecture enables consistent performance across multiple platforms and facilitates straight forward software and policy maintenance.

Because the Viatores Server code baseline is already in Linux, the porting of Viatores Client to Linux is relatively simple and highly achievable, as well as to the Apple OS X platform which is already based on the BSD distribution and has many operating system calls similarity with Linux. Ecutel plans to develop Viatores Client for other platforms such as Linux and Apple OS X.

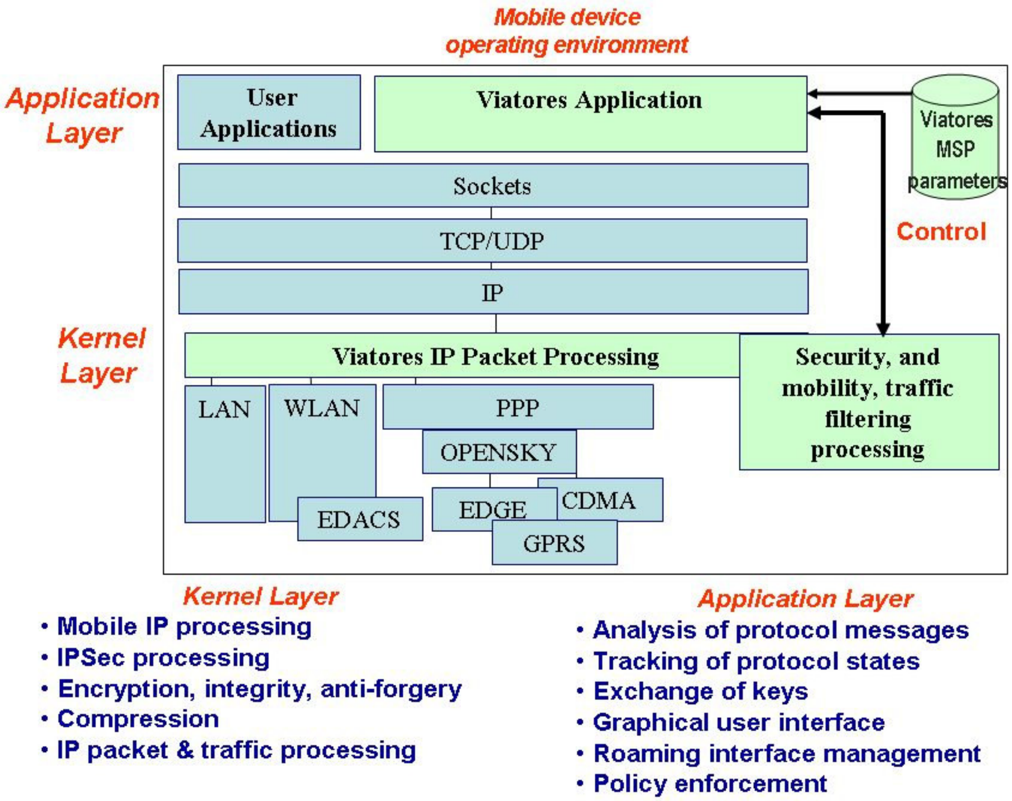

Mobile device operating environment
Application Layer
User Applications
Viatores Application
Viatores MSP parameters
Sockets
TCP/UDP
IP
Control
Kernel Layer
Viatores IP Packet Processing
Security, and mobility, traffic filtering processing
LAN
WLAN
PPP
OPENSKY
EDACS
EDGE
CDMA
GPRS
Kernel Layer
• Mobile IP processing
• IPSec processing
• Encryption, integrity, anti-forgery
• Compression
• IP packet & traffic processing
Application Layer
• Analysis of protocol messages
• Tracking of protocol states
• Exchange of keys
• Graphical user interface
• Roaming interface management
• Policy enforcement

Figure 5-9: Viatores Client architecture

5.10 Minimal Configuration and/or Intervention—-(Mandatory)

The client software must have pre-configurable parameters for ease of deployment. Vendors should explain how their product meets these criteria.

Ecutel Response: The Ecutel's Viatores solution complies with the minimal configuration and/or intervention requirement

The Viatores Client software provides a comprehensive set of capabilities to allow the Viatores system to automatically adhere to the system configured by the system administrator, at the same time, enables for system wide ease of deployment and maintenance.

These pre-configured parameters are the basis for Viatores Mobility and Security Policy (MSP). The Viatores Manager allows the system administrator to design and create MSP to efficiently control how the mobile device adheres to roaming priority, IP traffic security protection, network access authentication, allowed roaming zones, traffic shaping rules for slow bandwidth network traffic restriction, packet encapsulating action when traversing across public Network Address Translation (NAT) gateways, and secure firewall traversal at the enterprise side of the network.

Once the MSP policy is created, each user laptop will be able receive the policy and populate it in its own local storage for its own use – this process is termed client provisioning.

The system administrator can configure the following specific policy parameters to allow the Viatores Client to operate autonomously without user intervention:

- **User fixed or assigned IP address**
- **Mobile IP parameters and time interval for Mobile IP registration and authentication**
- **IP Security standard parameters and time interval for cryptographic key refresh and exchange**
- **Gateway and Server IP addresses**
- **Multiple roaming networks with IP addresses and netmask**
- **Default router IP address**
- **Split tunneling policy to allow traffic to be transmitted outside of Viatores secured tunnel, if enhanced throughput and performance is needed, over an active interface based on destination IP, protocol number, and port number**
- **Traffic control and shaping policy to ensure only specific application traffic can be transmitted on a specific network or interface**
- **Enable or disable user with privilege to modify or add local split tunneling policy**

These MSP parameters are persistent on the mobile device and are always accessible to the Viatores Client upon start-up and during run time. The system administrator always has access to the central MSP database located within the Viatores Manager to update and enable propagation of these MSP parameters to the end user mobile device whenever necessary.

In addition, the Viatores Client installation program is designed to run either in the interactive or silent (also known as batch mode) method. With the silent batch mode installation method, the system administrator can specify all necessary controlling parameters to enable the Microsoft Installation (MSI) to perform automatic software installation, update, patch and repair so that the files are maintained consistently, and at the same time, retain all administrator and user selected options as first installed on the mobile device to control how the user can access and operate the Viatores Client on the mobile device.

5.11 Retention of User Information—-(Mandatory)

The client software must be configurable to retain user specific information. Vendors should explain how their product meets these criteria.

Ecutel Response: The Ecutel's Viatores solution complies with the retention of user information requirement

The Viatores Client software provides a comprehensive set of capabilities to adhere to system security parameters configured by the system administrator as well as to allow the user with sufficient privilege to augment with user specific configuration.

The system administrator can configure the following policies to allow the Viatores Client to retain it on the laptop computer:

- **User login name**
- **User fixed or assigned IP address**
- **Mobile IP and IP Security parameters**
- **Gateway and Server default mobility Servers**
- **Enable or disable the viewing of user interface on the Viatores Client**
- **Split tunneling policy**
- **User credential authentication type that must be entered in order to gain access to the Viatores network**
- **Enable or disable user with privilege to modify or add local traffic shaping or traffic control policy**
- **Enable or disable user with privilege to modify or add local split tunneling policy**

In addition to these system configuration parameters, the user can enter the following parameters and instruct the Viatores client software to store it locally in the same set of configuration locations for reuse, such as in the Registry and the local binary encrypted files:

- **Set Hotspot detection and hotspot access search interval**
- **Save user password with strong encryption on the local machine for reuse during login to provide quick launch of the Viatores Client**
- **Change Viatores start-up mode from manual to automatic upon laptop login**
- **Change display log to vary with information between minimum and very detail levels**
- **Add local split tunnel policy to enable local traffic filtering, only if this option is enabled by the MSP parameters and the system administrator (such as local printing, search the web without having to traverse the secured tunnel to the enterprise network firewall)**
- **Retrieve and save multiple local MSP policies for more than one user so that they can share the same mobile device and use different login credentials to gain access to the network**

The Viatores Manager is a powerful tool to create the MSP parameters that guide all automated mobility and security operations within the Viatores system. It also can be used to enable specific Viatores users with additional localized capabilities to customize

their Viatores mobile operating environments to better suit their unique missions and communication requirements.

5.12 Enterprise Configuration and Management

Explain any enterprise configuration and management abilities available for your software. Does the system support central management of all remote users? How many mobile device connections does the system support? Does the system have redundancy? What technique does the system use to keep track of the mobile client as it moves from IP network to IP network? Does the system support single sign-on capabilities? Does the system support remote monitoring to check the status of all connected devices?

Ecutel Response: The Ecutel's Viatores solution complies with the enterprise configuration and management requirement

Viatores strength in client secure roaming starts with the Viatores Manager, which is a centralized system manager with flexible capabilities to provision and enable the Client and Server component with pre-configuration Mobility and Security Policy (MSP) parameters. The Viatores Configuration Manager and installation Manager can generate policy parameters for the following categories.

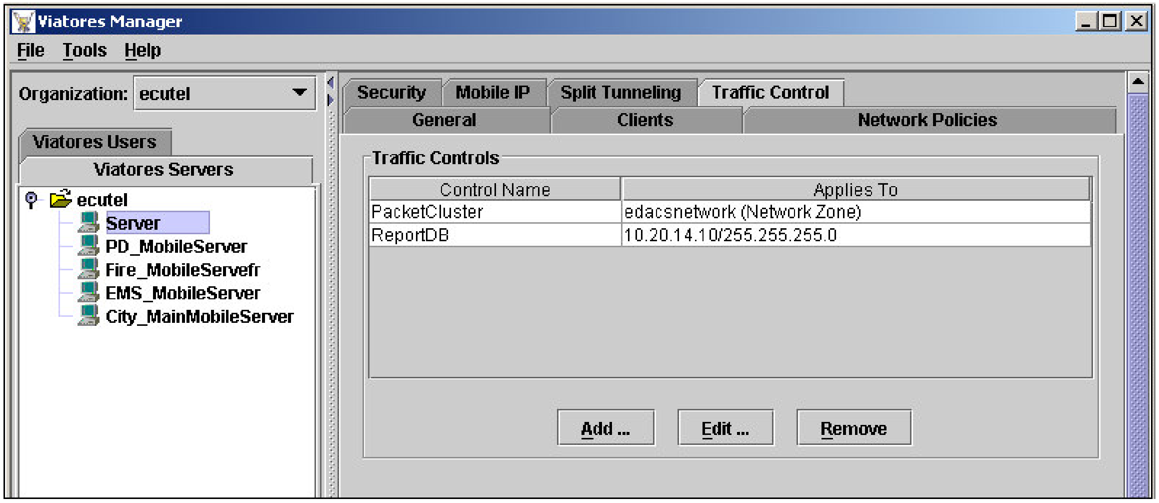
Category	Component	Capabilities	Specific parameters and options
Deployment topology	**Server and Client**	**Server IP, Gateway IP, Fail-over, router IP, netmask**	**For automatic IP packet header formation to send between Client, Gateway, Server**
	Server and Client	**IP address range to assign to mobile Client, DNS IP, WINS IP**	**To allow Client to maintain Mobile IP persistent IP address and to gain access to network**
Roaming	**Client, Server, Gateway**	**IP subnet and network specification**	**Enable and disable Client roaming into certain network and subnet zones to prevent security compromise. Detect commercial Wi-Fi Hotspot for ease of access**
	Client	**IP traffic Shaping, Control and Filter for attached network type, IP destination, protocol, port number**	**Enable and disable certain traffic transmission based on network type to control network traffic to prevent link overloading**

Category	Component	Capabilities	Specific parameters and options
	Client	IP traffic Split-Tunnel for IP destination, protocol, port number	Enable and disable non-encrypted path for non-critical function such as printing, local resource access, web access
Security and Mobility	Client and Server	IKE main mode and quick mode parameters, key refresh interval. Registration interval	3-DES, AES, SHA-1, pre-shared keys, perfect-forward secrecy, X.509 digital certificate, MD-5, with interval from 60 seconds to a full day
Authentication	Client and Server	Simple or 2-factor authentication for user access	RADIUS, Active Directory, SecurID, LDAP, local database
Sign on	Client and Server	Control for always-on security	Single sign-on, manual, automatic Client start up, or restricted access, to gain access to network resources

Table 5-12: Policy configuration capability

After the Client and Server are loaded or configured with MSP parameters, all Viatores networking functions are automated such that, during the run time, the user simply provides authentication credential to activate mobile device's provisioned capabilities. These policy parameters are structured in terms of execution rules, are protected with encryption to avoid tempering, retain same configuration for reuse. The parameters can be processed by any compatible versions of Viatores Client and Server, thus improving software capability updates while minimizing maintenance requirements and user downtime.

Figure 5-12 shows a sample page of the Viatores Manager component that can centrally manage and provision mobility and security policies for multiple Viatores Servers, Client, groups and authentication schemes.



Organization: ecutel

Control Name	Applies To
PacketCluster	edacsnetwork (Network Zone)
ReportDB	10.20.14.10/255.255.255.0

Figure 5-12: Viatores Central Manager Component

With the addition of the cryptographic hardware acceleration, sufficient PCI bus speed and a sufficiently fast central processing unit (such as Intel 2 GHz processor), the Viatores Server can accommodate between 500 to 1000 concurrent users connections.

The Viatores Server can operate in a fail-over cluster in which each Server has two LAN interfaces. The first LAN interfaces process user traffic while the second LAN interface is used to maintain cluster heart beats and MIP and IPSec state transfer. One of the Servers operates as the primary node and the other serves as the back-up node. When the primary Server fails, the back-up node already contains all mobile device states and can immediately take over and process user traffic without disruption.

For tracking of mobile node IP addresses as the remote users move from network to network, the Viatores Client performs MIP registration according to the procedures described in the sections 5.15 and 5.16 to inform the Viatores their current IP location. Since the Server maintains latest IP address information, the Server can immediately forward traffic to the mobile device latest point of attachment.

As part of the Viatores Client security capability to authenticate user access to the laptop and to the domain, the Viatores Client prompts the user to enter Active Directory user credential (i.e. name, password and domain) and authenticate to the Active Directory domain. If that authentication is successful, then the Viatores Client will establish a MIP and IPSec tunnel to allow laptop login and subsequently log into the domain. As the result, the user has direct, secure and authenticated path to the network resources such as email, domain host access, mapped files, shared printer and so forth. Essentially, the Viatores system provides a logical secure connection to the enterprise network as if the mobile device physically connects to the network itself.

The Viatores Server's Mobile IP monitoring and logging capability allows the system administrator to view the following information about the users on the Server graphical user interface:

- **Number of Clients to monitor**
- **Current active and connected users**
- **Remote user permanent and care-of IP addresses**
- **Connection time, date and for how long**
- **IPSec Security key exchange last performed**
- **Mobile IP authentication last perform**
- **Authentication status and name of the user who authenticates to the system**

The logging information can be viewed locally or remotely. These files are archived on disk as the log file becomes large to a pre-determined size. In addition, the Server and its authentication traffic log files can be retrieved to generate report off-line for analysis and reporting purposes.

5.13 Manufacturer Independent Equipment—-(Mandatory)

Explain compatibility with vendor equipment for:

a. networking equipment in general;
b. 802.11 Access Points specifically; and,
c. access devices including PCs, laptops, and PDAs.

Ecutel Response: the Ecutel's Viatores solution, a suite of software components that is hardware independent, complies with the manufacturer independent equipment requirement

The Viatores high-level compatibility matrix is as follows:

Category	Type	Typical product name
Networking Equipment	IP Router, layer-3 switch, LAN, layer-2 switch, Wi-Fi	Cisco, 3-COM, Intel, HP, etc
Security	Firewall	Cisco Pix, Checkpoint, Netscreen, Raptor, Gauntlet, IPTables, etc
Environment	Operating system	MS 98, ME, 200, XP, 2003, PocketPC 2002/2003, Linux

Category	Type	Typical product name
Dial up	Modem	All standard modems (wired or wireless)
Network	Public and private	CDMA, GPRS, Ricochet, EDGE, EVDO, GSM, DSL, Cable, EDAS, Opensky, IPMobilenet, etc

The Viatores product suite interoperates with any IP based network equipment, such as IP router, switches, layer-3 switch, VLAN, LAN, wireless LAN, wireless WAN, firewall, NAT, NATP, proxy gateway, and laptops with an IP protocol stack. Ecutel feels very confident that the Viatores solution can interoperate with existing equipment currently deployed in the State of Utah network and does not require any specific hardware to enable its operation. Thus, the State of Utah users can manage and control the cost of hardware deployment and upgrade.

5.14 Novell Netware Compatible

The State has a large installed base of Novell Netware servers. The network persistence system must function with PCs and servers running Netware. Vendors should explain whether their system will work with Netware running on client PCs and, if not, whether there is a plan to make their software work with Netware in the future, including a time line for implementation of this plan.

Ecutel Response: The Ecutel's Viatores provides compatibility with the Novell Netware software

The Viatores Client is able to intercept and process IP packets at the network layer 3.

During run time, the Novell Client's traffic runs at the application level and binds to the permanent IP address assigned to the Viatores Virtual Adapter. When Novell Client sends its traffic, the Viatores protocol driver will capture these UDP/TCP packets and process them through the mobility and security policy to send to the Viatores Server. At the Viatores Server, such traffic is de-capsulated, validated, decrypted and subsequently forwarded to the Novell server for further processing.

The Viatores Client and Server drivers act as two end points of the mobile user's secure tunnel to transmit Novell traffic transparently.

When the Novell servers transmit traffic back to the Client, the Viatores Server will intercept such traffic since it is destined to the Client's fixed IP address. The Server will process Client's traffic through the mobility and security policy and forward it back to the Viatores Client. The Viatores Client driver will de-capsulate, validate, decrypt and forward original traffic back to the Novell Client.

5.15 IP Mobile Standards

Does the system utilize the Mobile IP standard to provide seamless mobility and static IP address support? Does the system automatically manage IP address changes and maintain session connectivity as mobile devices move between subnets? Please explain.

Ecutel Response: The Ecutel's Viatores solution implements the Internet Engineering Task Force (IETF) Mobile IP standard to provide optimized heterogeneous network roaming, connection management and automated traffic tunneling

Viatores implements Mobile IP as the core protocol to enable mobile devices with seamless roaming over any layer-2 communication interface at the same time maintains a persistent IP address on the protocol stack. Upon start-up, the Viatores Client makes use of the pre-configured MIP parameters to configure the Viatores NDIS Virtual Adapter with a permanent IP address, which is uniquely assigned to each mobile user by the Viatores Manager and Server. The Viatores Client, the Virtual Adapter and the Mobile IP protocol driver operate in synchronization to maintain the proper network IP route entries, the Address Resolution Table (ARP) table, network route preferences, and multiple dynamic IP addresses acquired by LAN or dial-up interfaces.

The Viatores Client performs Mobile IP registration with the Viatores Server at pre-configured intervals or when the Client switches to a new network or obtains a different IP address on the current active interface. Each time a mobile device roams to a network, the roaming interface will be dynamically assigned an IP address by DHCP or PPP. After the new IP address is acquired, the Viatores Client will send a Mobile IP registration in UDP format to the Viatores Server, also to the Viatores Gateway if the mobile device accesses a network outside of the enterprise environment, to inform them of its new care-of address (i.e. attachment point IP address). The Viatores Server and Gateway respond to the Client's roaming event by updating the Client's care-of address in its local database. As a result, the Client, Server and Gateway maintain a new Mobile IP tunnel state to accommodate further traffic. Each time a Mobile IP registration is sent to the Server and Gateway and is processed successfully according to the Mobile IP standard, the Server and Gateway will renew its internal registration interval, storage maintenance and record keeping until either that time interval lapses or Client deregisters, which is the signal for the Server and Gateway to stop maintaining Mobile IP states of the mobile users.

In the kernel level, the Viatores Client always maintains one persistent IP address and multiple dynamic IP addresses (one for each active interface). Based on MSP parameters, there will be one selected transmission path between the Viatores Client and the Viatores Server to exchange tunneled traffic. Each time the mobile device roams to a new network that assigns dynamic IP address, the Viatores Client driver will reassign and maintain internally that new IP address for that particular communication interface. Similarly, when the mobile device roams to the new network whose interface already holds a fixed IP address, such as for the EDACS or CDPD network, the Viatores

Client driver will continue to make use of that same IP and marks the interface as current and activate it to maintain continuous tunneled traffic with the Viatores Server.

To maintain a continuous stream of traffic with the enterprise network, the Viatores Client detects and activate the proper Viatores MSP rules and parameters depending on the network connection IP address and whether the laptop has one or more active network interfaces. These MSP rules allow the Client to choose the best interface, use proper IP encapsulation, with either Mobile IP IP-in-IP or UDP header, to protect and transmit IP traffic across the public network and private network that may lead to a Network Address Translation (NAT) gateway.

To clarify the strength of dynamic header encapsulation of Viatores using Mobile IP standard, please see the following example depicted in the figure 5-15. This figure shows that the mobile device has 2 interfaces – CDMA and 802.11 – where the CDMA acquires an IP address (e.g. 16.23.45.123) and the wireless LAN acquires a private IP address (e.g. 10.20.30.2). Due to the use of connection prioritization policy, the Viatores Client selects the wireless LAN connection due to its speed and exchanges traffic with the enterprise network using UDP encapsulated method. When the mobile user moves outside of the wireless LAN coverage, the Viatores Client detects a drop in the 802.11 connection and resorts to the always-on CDMA connection. However, at this time the Viatores Client will use a more efficient IP-in-IP encapsulation to exchange traffic with the enterprise network. In both cases, the Viatores Client will send traffic to the right Gateway IP address or Gateway Server IP address, even traversing across the firewall, to make sure the end-to-end mobility states are established quickly to accommodate application traffic transmission.

Because there are no changes in the network stack IP and route entries that affect applications due to Mobile IP protocol implementation, application sessions operating at the IP layer-4 and above can maintain their persistence before, during and after roaming across network interfaces across public and private network boundaries.

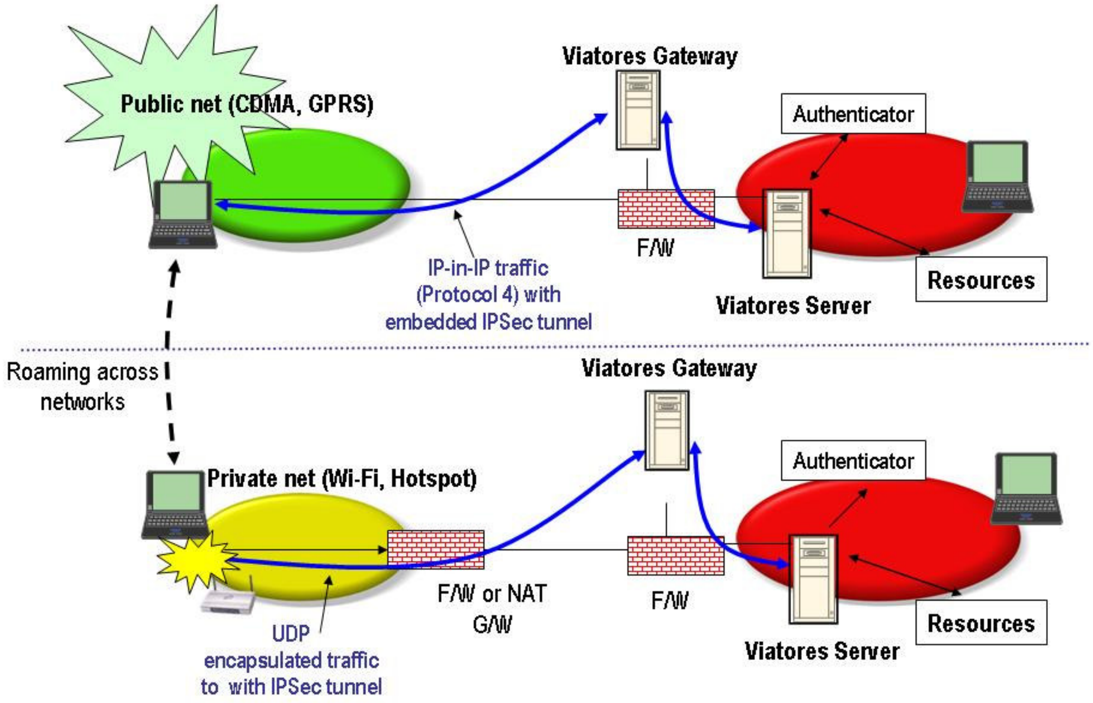


Figure 5-15: Dynamic IP encapsulation between the Mobile IP IP-in-IP and UDP methods without breaking the application session

5.16 Seamless Roaming—-(Mandatory)

Does the system allow mobile uses to roam freely and securely across wireless networks or among different network types (wired, wireless LAN, and wireless WAN) without disruption to applications?

Ecutel Response: The Ecutel's Viatores solution complies with requirement for seamless roaming across different networks without disruption to applications

The Viatores system implements standard Mobile IP and IPSec protocols to allow mobile users to roam freely and security across wired and wireless networks without disruption to applications and the secure tunnel while accessing one or more of these network types: CDMA, EVDO, GPRS, EDGE, GSM, cellular phone, 802.11a, 802.11b, 802.11g, DSL, Cable, analog modem, EDACS, Opensky, IP MobileNet, and so forth.

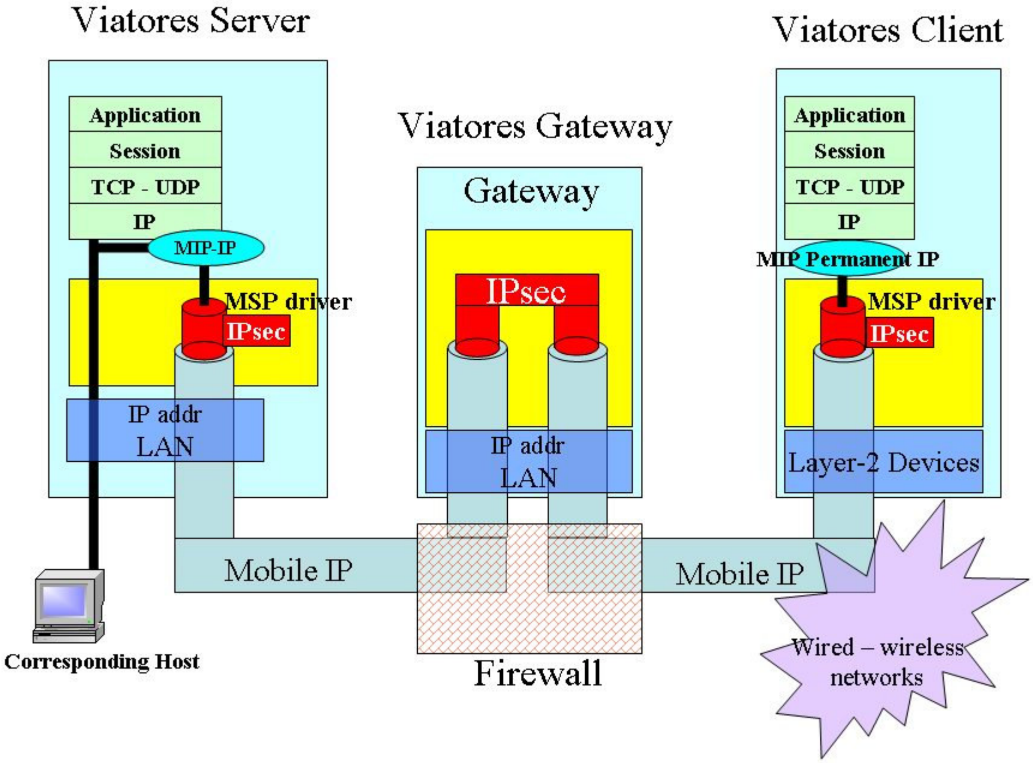


Figure 5-16.1: Mobile IP and IPSec tunnels to support secure and seamless roaming

The Viatores Client operates at IP layer-3 and higher, therefore it is agnostic about the underlying communication networks and can transmit IP traffic while controlling roaming over any of these interfaces. By strictly maintaining security and mobility policy that controls access to the enterprise network, the Viatores Client will properly establish authentication and association with the Viatores Server and Gateway to enable a continuous stream of traffic to flow to and from the mobile device.

Viatores provides seamless and secure roaming across different wired and wireless networks without disruption to applications by implementing policy driven layered mobility and security tunneling using the client and server architecture. The Viatores tunneling technology is operated on the Viatores Client component and on the Viatores Server and Gateway. The mobility control functions are implemented such that the Viatores Client can maintain constant mobility association with the Viatores Server and Gateway using Mobile IP registration and authentication. Each time the mobile device switches from one IP address to another during network roaming, the Viatores Client will immediately reestablish the mobility tunneling by informing the Gateway and Server its latest location. Thus the Gateway and Server can immediately and correctly transmit traffic to the right location of the mobile device. For more details on Viatores Mobile IP implementation, please see section 5.15.

After the mobility tunnel association is established, and this is usually when the user roams to or access remotely from outside of the enterprise network, the Viatores Client will validate the IP address of the currently active interface against the Viatores secured mobility protection policy to determine if IP security protection is necessary. If IP security is required, the Client will automatically create an IPSec security association through the use of IPSec key exchange and tunneling establishment process, as mentioned in section 5.8 Encryption and Security.

The Viatores Client, Gateway and Server establish the end-to-end LMS associations while temporarily holding application session traffic in their internal buffers until the tunneling operation is completed. Once the LMS tunneling is completed, the application traffic can be transmitted in both directions securely with encryption, anti-replay protection and anti-forgery protection.

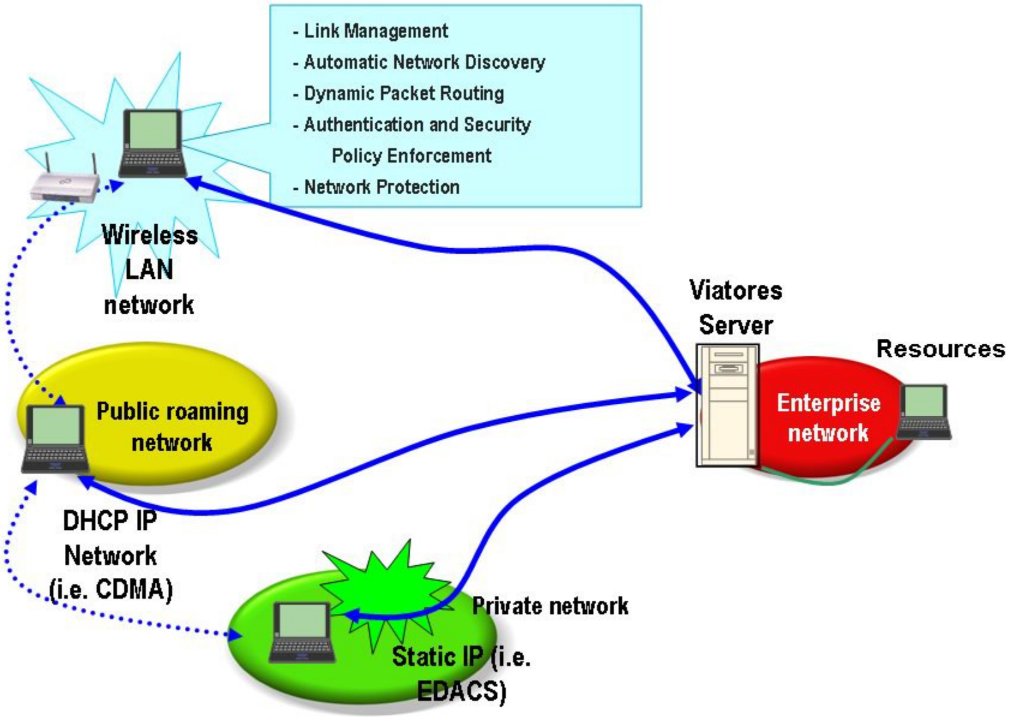


Figure 5-16.2: Viatores Client roams seamlessly across heterogeneous networks according to Viatores policy.

The Viatores policy actions are performed transparently to the application sessions to ensure they continue to persist, transmit and receive data, as well as are being protected from the underlying layer-2 network changes and with industry standard IP security for network traffic.

5.17 Network Switching Based on Bandwidth

Does the system have the ability to switch automatically to the fastest bandwidth network connection when multiple connections are active? Please explain.

Ecutel Response: The Ecutel's Viatores solution provides both automatic and user-driven manual methods to control network switching based on network characteristics

The Viatores Client provides automated network switching based on:

- **default network switching algorithm, and**
- **user defined network switch preference.**

With the default network switching algorithm, the Viatores Client prefers LAN and WLAN over PPP connection. This means if there are both an active NDIS LAN/WLAN and a dial-up connection, the Viatores Client will switches network traffic to the LAN/WLAN path; if the LAN'WLAN connection is dropped or disassociated with the LAN/WLAN port, the Viatores Client will seamlessly switch to the PPP connection to continue with packet transmission.

In addition to the predefined network preference algorithm, the user can override the Viatores default network switching by using the Viatores Adapter Prioritization Utility – see figure 5-17 for more detail - to rank switching preference based on communication type or name or speed. For example, if a mobile device has 3COM built-in LAN, Cisco WLAN 350, Verizon CDMA 2000, Bluetooth EDGE and dial-up modem, the user can rank switch as follows:

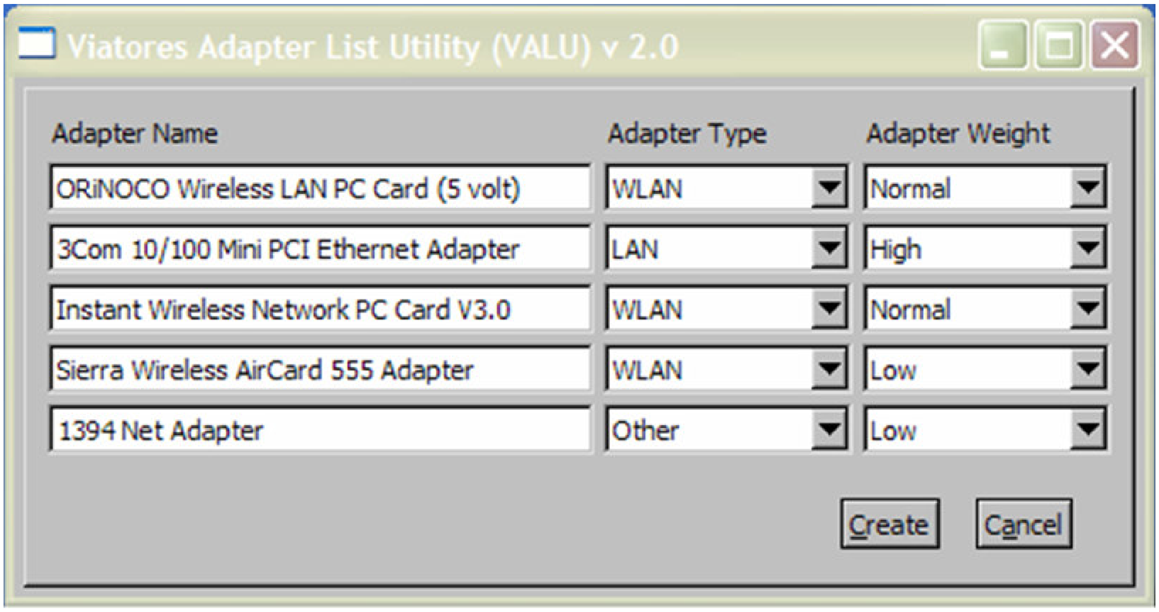
- **3COM built-in LAN (Treat as LAN - Most preferred)**
- **Cisco WLAN 350 (Treat as Wireless LAN - Most preferred)**
- **Verizon CDMA 2000 (Treat as Wireless LAN – Medium Preferred)**
- **Bluetooth EDGE 2000 (Treat as Wireless LAN – Least Preferred)**
- **modem (Treat as PPP – Medium Preferred)**

Based on the adapter prioritization list, the Viatores Client can automatically recognize the active network connections and selects a connection in a top-down fashion. If the chosen connection does not provide a successful communication path after a short trial interval (such as when cable is unplugged at the access point but the 802.11 signal is still strong), the Viatores Client will switch to the next one down from the list.

In another scenario, it is possible that the mobile device can be in a coverage area of both 802.11 and CDMA 2000, the Viatores Client will first select the 802.11 connection for data transmission. When the mobile device moves out of range of 802.11 coverage, the

Viatores Client will seamlessly and automatically switch to the CDMA 2000 connection to continue with data transmission.

Viatores Client's strength and flexibility in seamless roaming without disrupting application sessions and the permanent IP identity on the mobile device, while making sure of using the most efficient communication path to transmit only proper data types, provides a very easy to use and powerful user experience.



Adapter Name	Adapter Type	Adapter Weight
ORiNOCO Wireless LAN PC Card (5 volt)	WLAN	Normal
3Com 10/100 Mini PCI Ethernet Adapter	LAN	High
Instant Wireless Network PC Card V3.0	WLAN	Normal
Sierra Wireless AirCard 555 Adapter	WLAN	Low
1394 Net Adapter	Other	Low

Figure 5-17: Viatores Connection management tool

6.0 Pricing

6.2 Enterprise System Pricing

Provide a price for an enterprise system as identified in your technical offer, as well as pricing for stand-alone systems should State agencies choose to implement a system separate from an ITS deployed system. This price must include the first year maintenance and support fees. Provide pricing as follows:

Ecutel Response:

Client Licensing Fee (with 1st year maintenance)	Total	25 Client Pack Pricing*
Licensing Fee for up to 100 clients:	$ 10,436	$ 2,609
Licensing Fee for up to 500 clients:	$ 50,860	$ 2,543
Licensing Fee for up to 1000 clients:	$ 99,120	$ 2,478
Licensing Fee for up to 5000 clients:	$ 482,600	$ 2,413
Licensing Fee for up to 10,000 clients:	$ 939,200	$ 2,348
Licensing Fee Application Hosting Software:	$ 10,000	
System Hardware:		
Other: Acceleration PCI card (SafeXcel™ 241-PCI)/each	$ 1,000	

***Client software licenses sold in blocks of 25**

6.3 Ongoing Maintenance and Support

Provide pricing for maintenance and support fees for second year, and for the three optional renewal periods of product license.

Ecutel Response:

The maintenance fee is based on total software deployed per location and includes both support and upgrades. The first year's maintenance is included in the above pricing. These discounts are applied when purchasing maintenance with the original Purchase Order.

One Year Prepaid (Second year)	**18% per year**
Two Years Prepaid (Second & Third Year)	**15% per year**
Three or More Years Prepaid (Fourth Year or more)	**10% per year**

6.4 Training

Provide pricing for any training recommended. Specify location, rates, and incidental costs.

Ecutel Response:

Ecutel Systems, Inc. offers the Viatores Basic Class. On-site training is provided by the professional consulting services organization and is available plus travel and expenses.

Viatores Basic Technical Training course: Provide an overview of networking protocol standards (MIP, IPSec, Routing, DHCP, PPP, Wired and Wireless protocols); Viatores components; Viatores mobility, security and connectivity capabilities; Administrator and User configuration, product installation and fielding; hands-on class room practice. This is a 2 day class.

On Site Training	**$ 1,000/day***
Headquarters Training	**$ 500/day**

Headquarters Address
Ecutel Systems, Inc.
2300 Corporate Park Drive Suite 410
Herndon, VA 20171

Professional Services (i.e. installation, training and consulting) does not include travel and other expense. All travel will be invoiced at cost based on travel from our Virginia office. With any Purchase Order over $25,000, the travel fee will be waived for professional services for the first site visit.

6.5 Consulting Services

If consultant services are offered to support the software, list the name, job title, and hourly rate for any proposed consultant:

Ecutel Response:

Name: Mark Mazur	**Title: Project Engineer**	**$ 1,500/day on site***
Name: Dzung Tran	**Title: CTO/Custom Development**	**$ 200/ hour headquarters**

Professional Services (i.e. installation, training and consulting) does not include travel and other expense. All travel will be invoiced at cost based on travel from our Virginia office. With any Purchase Order over $25,000, the travel fee will be waived for professional services for the first site visit.

Glossary of Terms

Term	**Definition**
3DES	Triple Data Encryption Standard
802.1x	IEEE standard for port access control
ADA	Americans With Disabilities Act
ACS	Secure Access Control Server
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
ASCII	American National Standard Code for Information Interchange
AVL	Automated Vehicle Location system
BMP	Windows Bitmap graphics format
CA	Certificate Authority
CAD	Computer Aided Dispatch system
CDMA	Code Division Multiple Access
CDPD	Cellular Digital Packet Data
DBMS	Data Base Management System
DHCP	Dynamic Host Configuration Protocol
DSA	Digital Signature Algorithm
DSL	Digital Subscriber Line
EAP	Extensible Authentication Protocol
EAP-TLS	EAP using Transport Layer Security
EAP-TTLS	EAP using Tunnel Transport Layer Security
EDACS	Enhanced Digital Access Communication System
EDGE	Enhanced Data GSM Environment
EMS	Emergency Medical Services
EMT	Emergency Medical Technician
EVDO	CDMA Evolution Data Only (high speed)
FTP	File Transfer Protocol
GIS	Geographic Information System
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
HazMat	Hazardous Materials
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange handshake for IPSec protocol
IKE main mode	IPSec IKE phase 1 of the key handshake
IKE quick mode	IPSec IKE phase 2 of the key handshake
IP	Internet Protocol Address
IPSec	Internet Protocol Security
ITU	International Telecommunication Union
IT	Information Technology
JPEG	Joint Photographic Experts Group (image compression)
LAN	Local Area Network
LDAP	Light Weight Directory Access Protocol

MAC	Media Access Control
MD-5	Message Digest 5 algorithm to create digital signature
MIP	Mobile Internet Protocol
MSP	Viatores Mobility and Security Policy
NAT	Network Address Translation
NAPT	Network Address and Port Translation
NDIS	Network Driver Interface Specification
NDS	Novell Directory Service
NTP	Network Time Protocol
ODBC	Open Database Connectivity
Offeror	Any entity submitting a response to this RFP
OpenSky	Wireless Private Network by M/A-COM
PCMCIA	Personal Computer Memory Card International Association
PKI	Public Key Infrastructure
PTT-ID	Push to Talk ID
RADIUS	Remote Authentication Dial-in User Service
RAID	Redundant Array of Independent Disks.
RDBMS	Relational Data Base Management System
RF	Radio Frequency
RFP	Request for Proposal, or this document
RMS	Records Management System
RSA	Rivest Shamir Aldelman public / private algorithm
SecurID	Token based authentication product from RSA
SNPP	Simple Network Paging Protocol
SNTP	Simple Network Time Protocol
SSL	Secure Socket Layer
SSM	System Status Management (CAD)
SQL	Structured Query Language
TCP/IP	Transmission Control Protocol/Internet Protocol
TDD	Telecommunications Device For the Deaf
TIF	Tag Image File
WAN	Wide Area Network
WCTP	Wireless Communications Transfer Protocol
Wi-Fi	Wireless Fidelity – referring to wireless LAN
WLAN	Wireless LAN
WPA	Wi-Fi Protected Access
WWAN	Wireless WAN
X.509	Standard for digital certificate, an ITU recommendation